Department of the Interior

Security Control Standard

System and Communications Protection

January 2012

Version: 1.2

Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	**Date:**

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	February 3, 2011	Initial draft
Timothy Brown	0.2	February 4, 2011	Incorporated comments into body text
Timothy Brown	1.0	February 17, 2011	Final review and version change to 1.0
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1
Lawrence K. Ruffin	1.2	January 18, 2012	Revised SC-13 to require control enhancement 1 for all information systems

TABLE OF CONTENTS

SECURITY CONTROL STANDARD: SYSTEM AND COMMUNICATIONS PROTECTION

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 System and Communications Protection (SC) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and communications protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary.

The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and communications protection policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** SC-1	**MOD** SC-1	**HIGH** SC-1

SC-2 APPLICATION PARTITIONING

Applicability: Moderate and High Impact Information Systems

Control: The information system separates user functionality (including user interface services) from information system management functionality.

Supplemental Guidance: Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical and is accomplished by using different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate. An example of this type of separation is observed in web administrative interfaces that use separate authentication methods for users of any other information system resources. This may include isolating the administrative interface on a different domain and with additional access controls.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-2	**HIGH** SC-2

SC-3 SECURITY FUNCTION ISOLATION

Applicability: High Impact Information Systems

Control: The information system isolates security functions from nonsecurity functions.

Supplemental Guidance: The information system isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions and domains) that controls access to and protects the integrity of, the hardware, software, and firmware that perform those security functions. The

information system maintains a separate execution domain (e.g., address space) for each executing process. Related control: SA-13.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SC-3

SC-4 INFORMATION IN SHARED RESOURCES

Applicability: Moderate and High Impact Information Systems

Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

Supplemental Guidance: The purpose of this control is to prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. Control of information in shared resources is also referred to as object reuse. This control does not address: (i) information remanence which refers to residual representation of data that has been in some way nominally erased or removed; (ii) covert channels where shared resources are manipulated to achieve a violation of information flow restrictions; or (iii) components in the information system for which there is only a single user/role.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-4	**HIGH** SC-4

SC-5 DENIAL OF SERVICE PROTECTION

Applicability: All Information Systems

Control: The information system protects against or limits the effects of the following types of denial of service attacks: all flaw-based, SYN flood, ICMP flood, UDP flood, teardrop, application-level flood, nuke and SQL injection attacks.

Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service

attacks. Employing increased capacity and bandwidth combined with service redundancy may reduce the susceptibility to some denial of service attacks. Related control: SC-7.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

P1	**LOW** SC-5	**MOD** SC-5	**HIGH** SC-5

SC-6 RESOURCE PRIORITY

Applicability: Moderate and High Impact Information Systems

Control: The information system limits the use of resources by priority.

Supplemental Guidance: Priority protection helps prevent a lower-priority process from delaying or interfering with the information system servicing any higher-priority process. This control does not apply to components in the information system for which there is only a single user/role.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** **SC-6**	**HIGH** **SC-6**

SC-7 BOUNDARY PROTECTION

Applicability: All Information Systems

Control: The information system:

a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and
b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Supplemental Guidance: Restricting external web traffic only to organizational web servers within managed interfaces and prohibiting external traffic that appears to be spoofing an internal address as the source are examples of restricting and prohibiting communications. Managed interfaces employing boundary protection devices include, for example, proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in an effective security architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ).

The organization considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third-party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-4, IR-4, SC-5.

Control Enhancements:

1. The organization physically allocates publicly accessible information system components to separate subnetworks with separate physical network interfaces.

   Enhancement Supplemental Guidance: Publicly accessible information system components include, for example, public web servers.

2. The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.

3. The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.

   Enhancement Supplemental Guidance: The Trusted Internet Connection (TIC) initiative is an example of limiting the number of managed network access points.

4. The organization:

   a. Implements a managed interface for each external telecommunication service;
   b. Establishes a traffic flow policy for each managed interface;
   c. Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted;
   d. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;
   e. Reviews exceptions to the traffic flow policy at least annually; and
   f. Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.

5. The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).
6. The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.

7. The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.

   Enhancement Supplemental Guidance: This control enhancement is implemented within the remote device (e.g., notebook/laptop computer) via configuration settings that are not configurable by the user of that device. An example of a non-remote communications path from a remote device is a

virtual private network. When a non-remote connection is established using a virtual private network, the configuration settings prevent *split-tunneling*. Split tunneling might otherwise be used by remote users to communicate with the information system as an extension of that system and to communicate with local resources such as a printer or file server. Since the remote device, when connected by a non-remote connection, becomes an extension of the information system, allowing dual communications paths such as split-tunneling would be, in effect, allowing unauthorized external connections into the system.

8. The information system routes [*Assignment: organization-defined internal communications traffic*] to [*Assignment: organization-defined external networks*] through authenticated proxy servers within the managed interfaces of boundary protection devices.

   Enhancement Supplemental Guidance: External networks are networks outside the control of the organization. Proxy servers support logging individual Transmission Control Protocol (TCP) sessions and blocking specific Uniform Resource Locators (URLs), domain names, and Internet Protocol (IP) addresses. Proxy servers are also configurable with organization-defined lists of authorized and unauthorized websites.

12. The information system implements host-based boundary protection mechanisms for servers, workstations, and mobile devices.

    Enhancement Supplemental Guidance: A host-based boundary protection mechanism is, for example, a host-based firewall. Host-based boundary protection mechanisms are employed on mobile devices, such as notebook/laptop computers, and other types of mobile devices where such boundary protection mechanisms are available.

13. The organization isolates [*Assignment: organization defined key information security tools, mechanisms, and support components*] from other internal information system components via physically separate subnets with managed interfaces to other portions of the system.

18. The information system fails securely in the event of an operational failure of a boundary protection device.

    Enhancement Supplemental Guidance: Fail secure is a condition achieved by the application of a set of information system mechanisms to ensure that in the event of an operational failure of a boundary protection device at a managed interface (e.g., router, firewall, guard, application gateway residing on a protected subnetwork commonly referred to as a demilitarized zone), the system does not enter into an unsecure state where intended security properties no longer hold. A failure of a boundary protection device cannot lead to, or cause information external to the boundary protection device to enter the device, nor can a failure permit unauthorized information release.

References: FIPS Publication 199; NIST Special Publications 800-41, 800-77.

Priority and Baseline Allocation:

P1	**LOW** SC-7	**MOD** SC-7 (1) (2) (3) (4) (5) (7) **(8) (12) (13) (18)**	**HIGH** SC-7 (1) (2) (3) (4) (5) (6) (7) (8) **(12) (13) (18)**

SC-8 TRANSMISSION INTEGRITY

Applicability: Moderate and High Impact Information Systems

Control: The information system protects the integrity of transmitted information.

Supplemental Guidance: This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-17, PE-4.

Control Enhancements:

1. The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.

   Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems. Related control: SC-13.

References: FIPS Publications 140-2, 197; NIST Special Publications 800-52, 800-77, 800-81, 800-113; NSTISSI No. 7003.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-8 (1)	**HIGH** SC-8 (1)

SC-9 TRANSMISSION CONFIDENTIALITY

Applicability: Moderate and High Impact Information Systems

Control: The information system protects the confidentiality of transmitted information.

Supplemental Guidance: This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-17, PE-4.
Control Enhancements:

1. The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by protective distribution systems.

   Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems. Related control: SC-13.

References: FIPS Publications 140-2, 197; NIST Special Publications 800-52, 800-77, 800-113; CNSS Policy 15; NSTISSI No. 7003.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-9 (1)	**HIGH** SC-9 (1)

SC-10 NETWORK DISCONNECT

Applicability: Moderate and High Impact Information Systems

Control: The information system terminates the network connection associated with a communications session at the end of the session or after thirty minutes of inactivity for all RAS-based sessions; thirty to sixty minutes of inactivity for non-interactive users. Long running batch jobs and other operations are not subject to this time limit.

Supplemental Guidance: This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating-system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. The time period of inactivity may, as the organization deems necessary, be a set of time periods by type of network access or for specific accesses.

Control Enhancements: None.

References: OMB Memorandums 06-16, 07-16; Federal Risk and Authorization Management Program (FedRAMP) Cloud Computing Security Requirements Baseline.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** SC-10	**HIGH** SC-10

SC-11 TRUSTED PATH

Applicability: Moderate and High Impact Information Systems

Control: The information system establishes a trusted communications path between the user and the following security functions of the system: [*Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication*].

Supplemental Guidance: A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD SC-11**	**HIGH SC-11**

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Applicability: All Information Systems

Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system.

Supplemental Guidance: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. In addition to being required for the effective operation of a cryptographic mechanism, effective cryptographic key management provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users.

Control Enhancements:

1. The organization maintains availability of information in the event of the loss of cryptographic keys by users.
2. The organization produces, controls, and distributes symmetric cryptographic keys using NIST-approved key management technology and processes.
5. The organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.

References: NIST Special Publications 800-56, 800-57.

Priority and Baseline Allocation:

P1	**LOW** SC-12	**MOD** SC-12 **(2) (5)**	**HIGH** SC-12 (1) **(2) (5)**

SC-13 USE OF CRYPTOGRAPHY

Applicability: All Information Systems

Control: The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Supplemental Guidance: None.

Control Enhancements:

1. The organization employs, at a minimum, FIPS-validated cryptography to protect unclassified information.

References: FIPS Publication 140-2; Web: CSRC.NIST.GOV/CRYPTVAL, WWW.CNSS.GOV.

Priority and Baseline Allocation:

P1	**LOW** SC-13 (1)	**MOD** SC-13 (1)	**HIGH** SC-13 (1)

SC-14 PUBLIC ACCESS PROTECTIONS

Applicability: All Information Systems

Control: The information system protects the integrity and availability of publicly available information and applications.

Supplemental Guidance: The purpose of this control is to ensure that organizations explicitly address the protection needs for public information and applications with such protection likely being implemented as part of other security controls.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** SC-14	**MOD** SC-14	**HIGH** SC-14

SC-15 COLLABORATIVE COMPUTING DEVICES

Applicability: All Information Systems

Control: The information system:

a. Prohibits remote activation of collaborative computing devices; and
b. Provides an explicit indication of use to users physically present at the devices.

Supplemental Guidance: Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

P1	**LOW** SC-15	**MOD** SC-15	**HIGH** SC-15

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Applicability: Moderate and High Impact Systems
Control: The organization issues public key certificates under an [*Assignment: organization-defined certificate policy*] or obtains public key certificates under an appropriate certificate policy from an approved service provider.

Supplemental Guidance: For user certificates, each organization attains certificates from an approved, shared service provider, as required by OMB policy. For federal agencies operating a legacy public key infrastructure cross-certified with the Federal Bridge Certification Authority at medium assurance or higher, this Certification Authority will suffice. This control focuses on certificates with a visibility external to the information system and does not include certificates related to internal system operations, for example, application-specific time services.

Control Enhancements: None.

References: OMB Memorandum 05-24; NIST Special Publications 800-32, 800-63.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-17	**HIGH** SC-17

SC-18 MOBILE CODE

Applicability: Moderate and High Impact Information Systems

Control: The organization:

a. Defines acceptable and unacceptable mobile code and mobile code technologies;
b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c. Authorizes, monitors, and controls the use of mobile code within the information system.

Supplemental Guidance: Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the system if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Policy and procedures related to mobile code, address preventing the development, acquisition, or introduction of unacceptable mobile code within the information system.

Control Enhancements:

4. The information system prevents the automatic execution of mobile code in [*Assignment: organization-defined software applications*] and requires [*Assignment: organization-defined actions*] prior to executing the code.

Enhancement Supplemental Guidance: Actions required before executing mobile code, include, for example, prompting users prior to opening electronic mail attachments.

References: NIST Special Publication 800-28; NIST Special Publication 800-28; DOD Instruction 8552.01.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-18	**HIGH** SC-18 **(4)**

SC-19 VOICE OVER INTERNET PROTOCOL

Applicability: Moderate and High Impact Systems

Control: The organization:

a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
b. Authorizes, monitors, and controls the use of VoIP within the information system.

Supplemental Guidance: None.

Control Enhancements: None.

References: NIST Special Publication 800-58.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-19	**HIGH** SC-19

SC-20 SECURE NAME/ADDRESS RESOLUTION SERVICE (AUHTORITATIVE SOURCE)

Applicability: All Information Systems

Control: The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.

Supplemental Guidance: This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service. Digital signatures and cryptographic keys are examples of additional artifacts. DNS resource records are examples of authoritative data. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data. The DNS security controls are consistent with, and referenced from, OMB Memorandum 08-23.

Control Enhancements:

1. The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.

   Enhancement Supplemental Guidance: An example means to indicate the security status of child subspaces is through the use of delegation signer (DS) resource records in the DNS.

References: OMB Memorandum 08-23; NIST Special Publication 800-81.

Priority and Baseline Allocation:

P1	**LOW** SC-20 (1)	**MOD** SC-20 (1)	**HIGH** SC-20 (1)

SC-21 SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

Applicability: Moderate and High Impact Information Systems

Control: The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.

Supplemental Guidance: This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service. Digital signatures and cryptographic keys are examples of additional artifacts. DNS resource records are examples of authoritative data. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data. The DNS security controls are consistent with, and referenced from, OMB Memorandum 08-23.

Control Enhancements: None Mandated.

References: OMB Memorandum 08-23; NIST Special Publication 800-81.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-21	**HIGH** SC-21

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE

Applicability: Moderate and High Impact Information Systems

Control: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

Supplemental Guidance: A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility). With regard to role separation, DNS servers with an internal role, only process name/address resolution requests from within the organization (i.e., internal clients). DNS servers with an external role only process name/address resolution information requests from clients external to the organization (i.e., on the external networks including the Internet). The set of clients that can access an authoritative DNS server in a particular role is specified by the organization (e.g., by address ranges, explicit lists).

Control Enhancements: None.

References: NIST Special Publication 800-81.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-22	**HIGH** SC-22

SC-23 SESSION AUTHENTICITY

Applicability: Moderate and High Impact Information Systems

Control: The information system provides mechanisms to protect the authenticity of communications sessions.

Supplemental Guidance: This control focuses on communications protection at the session, versus packet, level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example, this control addresses man-in-the-middle attacks including session hijacking or insertion of false information into a session. This control is only implemented where deemed necessary by the organization (e.g., sessions in service-oriented architectures providing web-based services).

Control Enhancements: None Mandated.

References: NIST Special Publications 800-52, 800-77, 800-95.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-23	**HIGH** SC-23

SC-24 FAIL IN KNOWN STATE

Applicability: High Impact Information Systems

Control: The information system fails to a [*Assignment: organization-defined known-state*] for [*Assignment: organization-defined types of failures*] preserving [*Assignment: organization-defined system state information*] in failure.

Supplemental Guidance: Failure in a known state can address safety or security in accordance with the mission/business needs of the organization. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system. Failure in a known safe state helps prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information system state information facilitates system restart and return to the operational mode of the organization with less disruption of mission/business processes.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SC-24

SC-25 THIN NODES

Applicability: High Impact Information Systems

Control: The information system employs processing components that have minimal functionality and information storage.

Supplemental Guidance: The deployment of information system components with minimal functionality (e.g., diskless nodes and thin client technologies) reduces the need to secure every user endpoint, and may reduce the exposure of information, information systems, and services to a successful attack. Related control: SC-30.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SC-25

SC-27 OPERATING SYSTEM-INDEPENDENT APPLICATIONS

Applicability: High Impact Information Systems

Control: The information system includes: [*Assignment: organization-defined operating system-independent applications*].

Supplemental Guidance: Operating system-independent applications are applications that can run on multiple operating systems. Such applications promote portability and reconstitution on different platform architectures, increasing the availability for critical functionality within an organization while information systems with a given operating system are under attack.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SC-27

SC-28 PROTECTION OF INFORMATION AT REST

Applicability: Moderate and High Impact Information Systems

Control: The information system protects the confidentiality and integrity of information at rest.

Supplemental Guidance: This control is intended to address the confidentiality and integrity of information at rest in nonmobile devices and covers user information and system information. Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system. Configurations and/or rule sets for firewalls, gateways, intrusion detection/prevention systems, and filtering routers and authenticator content are examples of system information likely requiring protection. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate.

Control Enhancements:

1. The organization employs cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest unless otherwise protected by alternative physical measures.

References: NIST Special Publications 800-56, 800-57, 800-111.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-28	**HIGH** SC-28 **(1)**

SC-30 VIRTUALIZATION TECHNIQUES

Applicability: Moderate and High Impact Information Systems

Control: The organization employs virtualization techniques to present information system components as other types of components, or components with differing configurations.

Supplemental Guidance: Virtualization techniques provide organizations with the ability to disguise information systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-30	**HIGH** SC-30

SC-32 INFORMATION SYSTEM PARTITIONING

Applicability: Moderate and High Impact Information Systems

Control: The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.

Supplemental Guidance: Information system partitioning is a part of a defense-in-depth protection strategy. An organizational assessment of risk guides the partitioning of information system components into separate physical domains (or environments). The security categorization also guides the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components. Related controls: AC-4, SC-7.

Control Enhancements: None.

References: FIPS Publication 199.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-32	**HIGH** SC-32

SC-33 TRANSMISSION PREPARATION INTEGRITY

Applicability: High Impact Information Systems

Control: The information system protects the integrity of information during the processes of data aggregation, packaging, and transformation in preparation for transmission.

Supplemental Guidance: Information can be subjected to unauthorized changes (e.g., malicious and/or unintentional modification) at information aggregation or protocol transformation points.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SC-33